	Application #	10/531,431
RENEWED PETITION UNDER 37 C.F.R. § 1.47(a)		National Stage of PCT/GB03/004377
	Confirmation #	
	Filing Date	15 April 2005
	First Inventor	JEAL
	Art Unit	
	Examiner	
	Docket #	P08620US01/BAS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

S I R:

Pursuant to the provisions of 37 C.F.R. § 1.47(a), and in response to the Decision on Petition dated June 23, 2006, Applicants hereby resubmit their petition to have the Oath from one of the two inventors in the above case accepted in the absence of the Oath from the second inventor who has refused to sign an Oath of the above application, and ask for reconsideration of Applicants' previously filed Petition.

As was pointed out in the initial Petition, in the present case, Applicants have continuously made diligent attempts to obtain the signature of both of the inventors but have yet been unable to obtain the signature for the Oath from inventor George Mudie. In particular, as reflected in the Declaration included with the initial Petition, Applicants showed that the inventor George Mudie had previously been provided with a copy of the International application which was entered in the US as the above-identified national stage application, and was sent copies of the Assignment and Oath, but never executed or returned these documents. As also reflected in Applicants' prior Petition, it was pointed out that Mr. Mudie was a former employee of Assignee, but no longer works for the Assignee, and his departure from the company was not on good terms.

In its Decision on Petition, the Petitions examiner appears to have ignored the sworn testimony of the Declarant indicating that Mr. Mudie in fact had a complete copy of

the present application, and has held instead that Applicants have not shown that he had a copy of the application in his possession. Accordingly, the Decision indicated that Applicants had not provided sufficient proof that Mr. Mudie had received a copy of the Application.

In addition, the Decision on Petition indicated that Applicants had not complied with item (4) and alleged that the executed Declaration was not included with the petition. Once again, the Petitions Examiner is incorrect since the petition papers as filed did indeed include said executed declaration, as reflected in the copy of the Petition and stamped receipt attached hereto as Attachment 1. Accordingly, Applicants' previous submission was in compliance with item (4) as required under 37 CFR §1.47(a).

In any event, in light of the Decision on Petition, a copy of the compete specification and cover papers along with an Inventor's Oath and Assignment was sent to inventor Mudie at his last known address, and these documents were in fact received at that last known residence. Mr. Mudie also sent an E-mail following his receipt of the Specification and Declaration which indicated his continued unwillingness to execute the inventor's Declaration. See attached Declaration of B. Aaron Schulman and attachments. Accordingly, despite having received the specification and cover papers, Oath and Assignment, still no executed documents have been received by inventor Mudie who continues to refuse to execute the inventors' Oath with regard to the present application.

As required under 37 CFR §1.47(a), and as provided in Applicants' original petition thereunder, the last known addresses of the inventor George Mudie who refused to execute the Declaration is as follows:

George Mudie, 2 Lawrences Lane, Thatcham RG18 3 LF, Great Britain

Accordingly, under CFR § 1.47(a), Applicants have shown that inventor Mudie refuses to join in the application by submitting an executed Oath despite the diligent efforts

to have him do so, as reflected in the attached Declaration and attachments thereto which is sufficient to show the necessary facts regarding this refusal.
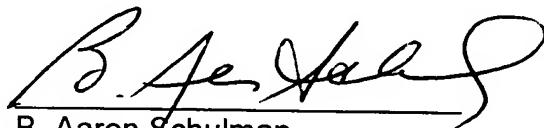
In light of the above evidence and the evidence provided herein, Applicants have provided the necessary information for the Patent Office to accept the Oath in this case from one of the two inventors pursuant to 37 CFR 1.47(a). Since the executed Declaration from inventor Jeal has been submitted and the required petition fee under 37 CFR 1.47(a) has been paid, reconsideration of the decision and granting of this petition is appropriate.

Should there be any questions, or should the Examiner require any additional information, a telephone call to the undersigned is welcomed.

Respectfully submitted,

STITES & HARBISON PLLC

Dated: August 23, 2006

B. Aaron Schulman
Registration No. 31877

1199 North Fairfax Street, Suite 900
Alexandria, Virginia 22314
(703) 739-4900

DECLARATION UNDER 37 C.F.R. § 1.47(a)	Application #	10/531,431 National Stage of PCT/GB03/004377
	Confirmation #	
	Filing Date	15 April 2005
	First Inventor	JEAL
	Art Unit	
	Examiner	
	Docket #	P08620US01/BAS

Commissioner for Patents
P.O. Box 1450
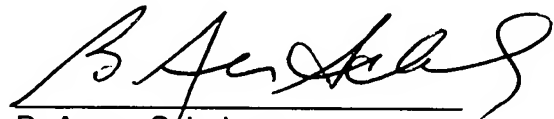Alexandria, VA 22313-1450

S I R:

On behalf of the Assignee of the present application, Vodafone Group Plc, the undersigned states that in order to obtain an executed Declaration in conjunction with the above application, I sent a copy of the complete patent application and cover papers as filed along with the Inventors' Oath and Assignment to inventor George Mudie via courier service (UPS) at his last known address, 2 Lawrences Lane, Thatcham RG18 3 LF, Great Britain. A copy of the letter and attachments is attached hereto as Appendix A. This package was delivered to Mr. Mudie at his last known address as reflected in the receipt from UPS attached hereto as Appendix B.

In response to receiving the Specification and Declaration, I received an E-mail from inventor Mudie indicating his continued unwillingness to execute the Inventor's Declaration for the present application. A copy of the E-mail received from inventor Mudie is attached hereto as Appendix C.

Despite having provided inventor Mudie with the complete copy of the application and cover papers field therewith along with the inventors' Oath and Assignment, no executed declaration has been received from inventor Mudie despite diligent efforts to obtain his executed Oath, and he continues to refuse to sign an Oath for the present application.

223LT:20285:20150:1A:ALEXANDRIA

I hereby state that all statements made herein based on my own personal knowledge are true and correct and that all statements based on my information and belief are true and correct to the best of my knowledge, and further that all of these statements have been made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Dated: August 23, 2006

B. Aaron Schulman
Registration No. 31877

1199 North Fairfax Street, Suite 900
Alexandria, Virginia 22314
(703) 739-4900

STITES & HARBISON PLLC

ATTORNEYS

1199 N. Fairfax Street
Suite 900
Alexandria, VA 22314
(703) 739-4900
(703) 739-9577 FAX
www.stites.com

July 28, 2006

B. Aaron Schulman
(703) 837-3907
(703) 518-2937 FAX
bschulman@stites.com

VIA COURIER

Mr. George Stronech Mudie
2 Lawrences Lane
Thatcham RG18 3 LF
GREAT BRITAIN

COPY

> **RE:** **JEAL et al - U.S. Appln. Serial No. 10/531,431**
> **Our Ref.: P08620US01/BAS**
> **C/M Code: 223LT-20285**

Dear Mr. Mudie:

I am the US patent attorney who is handling the above patent application in which you are named as an inventor. I have been asked to provide you with the patent application and inventors' Oath and Assignment documents in conjunction with the above case.

Accordingly, I am enclosing at this time a copy of the complete patent application and cover papers for the above case along with an inventors' Declaration and an Assignment. We would like you to execute and date the Declaration and Assignment, and forward the executed documents to this office for filing. If possible, please return the executed documents via facsimile at 703-739-9577. We would also request that you send us the executed originals via Courier, and we would be happy to provide you with our Courier information if you so dsesire.

We thus look forward to the return of the executed documents as soon as possible, and please do not hesitate to contact me should you have any questions. Thank you in advance for your assistance.
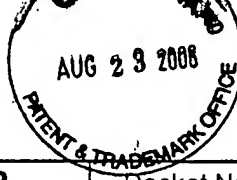
Sincerely,

STITES & HARBISON, PLLC

B. Aaron Schulman

BAS:smj
Enclosures

223LT:20285:34659:1:ALEXANDRIA

Customized PTO/SB/01 (09-04)

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

Docket No.	
1st Inventor	JEAL, David
	COMPLETE IF KNOWN

☐ Declaration Submitted **with** Initial Filing

☒ Declaration Submitted **after** Initial Filing

Appl. No.	
Filing Date	

I hereby declare that:

Each inventor's residence, mailing address and citizenship are as stated below next to their name.

I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

FACILITATING AND AUTHENTICATING TRANSACTIONS

the specification of which:

☐ is attached hereto
   OR

☒ was filed on 9 October 2003 as US Application No. or PCT International Application No. **PCT/GB2003/004377**
   and (if applicable) was amended on

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim FOREIGN PRIORITY benefits under 35 USC 119(a)-(d) or (f), or 365(b) of any foreign application for patent, inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the US, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's certificate, or any PCT international application having a filing date before that of the application on which priority is claimed. (☐ *Additional applications listed on supplemental sheet provided herewith*)

Prior Foreign Appl. No.	Country	Filing Date (MM/DD/YYYY)	Priority Not Claimed
0224228.7	GB	17 OCTOBER 2002	
0307248.5	GB	28 MARCH 2003	
0311729.8	GB	21 MAY 2003	

Power Of Attorney & Correspondence Address Indication

I hereby appoint the practitioners (of **Stites & Harbison PLLC**) associated with

CUSTOMER NUMBER 00881

as my/our attorneys or agents to prosecute the application identified above, and to transact all business in the US Patent and Trademark Office connected therewith.

Please **direct** all correspondence to the address of the above-mentioned Customer Number.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 USC 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon. (☐ *Additional inventors named on supplemental sheet provided herewith*)

SOLE OR FIRST INVENTOR		Citizenship	GB

Given Name (First and Middle [if any])	David	Family Name or Surname	JEAL
Full Mailing Address	8 Callow Croft , Burbage, Marlborough SN8 3TB, GREAT BRITAIN		
Residence - City, State/Country (if different from mailing address)	"same as above"		
SIGN AND DATE HERE	Inventor's Signature X /David/	Date x 26th MAY 2005	

SECOND JOINT INVENTOR (if any)		Citizenship	GB

Given Name (First and Middle [if any])	George Stronach	Family Name or Surname	MUDIE
Full Mailing Address	2 Lawrrences Lane, Thatcham RG18 3LF, GREAT BRITAIN		
Residence - City, State/Country (if different from mailing address)	"same as above"		
SIGN AND DATE HERE	Inventor's Signature X	Date X	

Stites & Harbison PLLC • 1199 North Fairfax Street • Suite 900 • Alexandria Virginia 22314
TEL (703) 739-4900 • FAX (703)-739-9577

223LT:0000:13972:1:ALEXANDRIA

ASSIGNMENT OF PATENT APPLICATION
(US and foreign rights - all rights assigned by inventors to a single assignee)

WHEREAS,
1) David Jeal 2) George Stronach Mudie

residing respectively at
1) 8 Callow Croft, Burbage, Marlborough SN8 3TB, GREAT BRITAIN
2) 2 Lawrences Lane, Thatcham RG18 3LF, GREAT BRITAIN

(hereinafter referred to as the "ASSIGNOR") has/have invented certain new and useful improvements in FACILITATING AND AUTHENTICATING TRANSACTIONS

for which an application for a United States Patent

    ☒ was executed on even date herewith
    was executed on
    was filed on   , as Serial No.:

And WHEREAS, VODAFONE GROUP PLC

whose Post Office Address is Vodafone House, The Connection, Newbury, Berkshire RG 14 2FN, GREAT BRITAIN

(hereinafter referred to as the "ASSIGNEE") is desirous of acquiring the entire right, title and interest in and to said application and the invention(s) and improvement(s) therein disclosed, for the United States of America or other countries, and any Letters Patent which may issue therefor in the United States or other countries including all divisions, continuations, reissues, renewals and/or extensions thereof.

NOW THEREFORE in consideration of the sum of ten U.S. dollars ($10.00) and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the ASSIGNOR does hereby assign, sell, transfer and set over unto the ASSIGNEE the entire right, title and interest in and to said application and the invention(s) and improvement(s) therein disclosed, for the United States of America or other countries, and any Letters Patent which may issue therefor in the United States or other countries and all divisions, continuations, reissues, renewals and/or extensions thereof, said ASSIGNEE to have and to hold the interests herein assigned to the full ends of the terms of said Letters Patent and any and all divisions, continuations, re-issues, renewals and/or extensions thereof, respectively, as fully and entirely as the same would have been held and enjoyed by the ASSIGNOR had this assignment not been made.
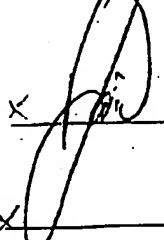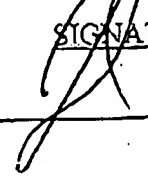
And for the consideration aforesaid, ASSIGNOR agrees that ASSIGNOR will communicate to said ASSIGNEE or the representatives thereof any facts known to ASSIGNOR respecting the invention(s) and improvement(s) of the said application(s), and will, upon request, but without expense to ASSIGNOR, testify in any legal proceedings, sign all lawful papers,

- 1 -

execute all divisional, reissue, continuation, renewal and/or extension applications, make all rightful oaths, and generally do all other and further lawful acts, deemed necessary or expedient by said ASSIGNEE or by counsel for said ASSIGNEE, to assist or enable said ASSIGNEE to obtain and enforce full benefits from the rights and interests herein assigned.

This assignment shall be binding upon the ASSIGNOR's heirs, executors, administrators, successors and/or assigns, and shall inure to the benefit of the heirs, executors, administrators, successors, and/or assigns, as the case may be, of the ASSIGNEE.

The Commissioner of Patents of the US is requested to issue such Letters Patent in accordance with this assignment.

I hereby authorize and request any attorney of record in said Application or any attorney of Stites & Harbison PLLC, Customer Nos. 00881, 24350 or 32885, to insert above any information concerning the identity of the parties or of said Application (including the serial no. and filing date).

NAME	SIGNATURE	DATE
1) David Jeal	X	X 26th MAY, 2005
2) George S. Mudie	X	X , 2005

	Application #	New US Application
	Confirmation #	
PRELIMINARY AMENDMENT	Filing Date	4/15/05
	First Inventor	JEAL et al.
	Art Unit	
	Examiner	
	Docket #	P08620US01/BAS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

S I R:

　　　　　Prior to examination, please amend the above-identified application as follows.

IN THE CLAIMS

Amendments to the Claims are reflected in the listing of the claims provided herewith in **Attachment A**.
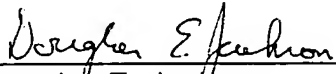
1

REMARKS

By this Amendment, the claims have been rewritten to reduce the multiple dependencies and to place the claims in better conformance with US practice. Further and favorable action is respectfully solicited.

Respectfully submitted,

STITES & HARBISON, PLLC

Date: 4/15/05

Douglas E. Jackson
Douglas E. Jackson
Registration No. 28518

1199 North Fairfax Street, Suite 900 - Alexandria, Virginia 22314 - (703) 739-4900

2

ATTACHMENT A
Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended)   A device ~~(30;250;270;290)~~ for connection to a data processing apparatus ~~(10)~~, the device including:

—first coupling means for operative coupling to authentication storage means ~~(12)~~ storing predetermined information relating to the authentication of a transaction with the data processing apparatus ~~(10)~~;

second coupling means ~~(34;254)~~ for operative coupling to the data processing apparatus ~~(10)~~, the device ~~(30;250;270;290)~~ when operatively coupled to the data processing apparatus ~~(10)~~ being responsive to an authentication process carried out via a communications link ~~(19)~~ for authenticating the transaction, the authentication process involving the use of the predetermined information;

and ~~characterized by~~ security data entry means ~~(46;276;296)~~ for obtaining security data independently of the data processing apparatus ~~(10)~~; and

means for storing the security data temporarily.

2. (Original)   The device of claim 1, wherein the security data is stored temporarily by means of a transient power source.

3. (Original)   The device of claim 2, wherein the transient power source comprises piezo electric means.

4. (Currently Amended)   The device of claim 3, wherein the piezo electric means comprises one or more piezo electric cells ~~(282)~~.

5. (Currently Amended) The device of claim 2, ~~3 or 4,~~ wherein the transient power source is charged by the security data entry means ~~(46;276;296)~~.

6. (Currently Amended) The device of claim 2, ~~3,4 or 5,~~ wherein the transient power source comprises a rechargeable battery.

7. (Currently Amended) The device of ~~any one of~~ claims 1 ~~to 6,~~ comprising means for analysing the entered security data for determining whether to allow access to the predetermined information.

8. (Currently Amended) A device ~~(250;270;290;310)~~ for connection to a data processing apparatus ~~(10)~~, the device ~~(46;276;296)~~ including:

first coupling means for operative coupling to authentication storage means ~~(12)~~ storing predetermined information relating to the authentication of a transaction with the data processing apparatus ~~(10)~~;

second coupling means ~~(254)~~ for operative coupling to the data processing apparatus ~~(10)~~; the device ~~(250;270;290;310)~~ when operatively coupled to the data processing apparatus ~~(10)~~ being responsive to an authentication process carried out via a communications link ~~(19)~~ for authenticating the transaction, the authentication process involving the use of the predetermined ~~configuration~~ information; and ~~characterized by~~ configuration means ~~(6)~~ for selectively rendering the second coupling means ~~(254)~~ available for coupling to the data processing apparatus ~~(10)~~.

9. (Currently Amended) The device of claim 8, wherein the configuration means comprises ~~(256;272;294;322)~~ means for selectively making the second coupling means ~~(254)~~ available externally of the device housing.

10. (Currently Amended) The device of claim 9, wherein the configuration means ~~(256;272;294;322)~~ comprises a removable cap.

11. (Currently Amended)   The device of claim 9, wherein the configuration means ~~(256;272;294;322)~~ comprises a closure member coupled to and moveable with respect to the housing for selectively closing an aperture in the housing.

12. (Currently Amended)   The device of claim 11, comprising interconnection means ~~(264,266)~~ for connecting the closure member and the second coupling means ~~(254)~~, the arrangement being such that, as the closure member is moved to open the aperture, the second coupling means ~~(254)~~ emerges from the aperture.

13. (Currently Amended)   The device of claim 8, comprising a knob mounted on the device housing for rotation with respect thereto, and means for converting rotation of said knob into linear movement of the second coupling means ~~(254)~~ such that rotation of said knob in a first direction causes the second coupling means ~~(254)~~ to emerge from an aperture in the device housing and rotation of said knob in a second direction causes the second coupling means to be retracted through said aperture.

14. (Currently Amended)   The device of claim 9, wherein the device housing includes two parts moveable with respect to one another between a first arrangement where the second coupling means ~~(254)~~ is contained within the housing and a second arrangement where the second coupling means is exposed for connection to the data processing apparatus.

15. (Currently Amended)   The device of claim 14, wherein the two parts are pivotally ~~(318)~~ coupled together.

16. (Currently Amended)   The device of ~~any one of~~ claims 8 ~~to 15~~, comprising security data entry means ~~(276;296)~~ for obtaining security data independently of the data processing apparatus ~~(10)~~, and means for analysing the entered security data for determining whether to allow access to the predetermined information.

17. (Currently Amended)   The device of ~~any one of~~ claims 8 ~~to 15~~, comprising security data entry means (276;296) for obtaining security data independently of the data processing apparatus;

223LT:20285:13616:1:ALEXANDRIA

and means for storing the security data temporarily.

18. (Currently Amended)   The device of ~~any one of~~ claims 1 ~~to 17~~, wherein the device controls access to the predetermined information.

19. (Currently Amended)   The device of ~~any one of~~ claims 1 ~~to 7 and to 18~~, wherein the security data entry means comprises alphanumeric data entry means.

20. (Currently Amended)   The device of ~~any one of~~ claims 1 ~~to 7 and~~ to ~~19~~, wherein the security data entry means comprises a keypad.

21. (Currently Amended)   The device of ~~any one of~~ claims 1 ~~to 7 and~~ to ~~20~~, wherein the security data comprise a Personal Identification Number (PIN) and analysing means compares the PIN obtained by the security data means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.

22. (Currently Amended)   The device of ~~any one of the preceding~~ claims 1, comprising a display ~~(48;248)~~ for displaying security information.

23. (Currently Amended)   The device of ~~any one of the preceding~~ claim 1, comprising a data processing module ~~(36)~~ for controlling the communication with the data processing apparatus ~~(10)~~.

24. (Currently Amended)   The device of claim 23, wherein the data processing module ~~(36)~~ of the device is configured for communicating with a corresponding data processing module ~~(38)~~ of the data processing apparatus ~~(10)~~.

25. (Currently Amended)   The device of claim 24, wherein communication between the authentication storage means ~~(12)~~ and the data processing apparatus ~~(10)~~ is performed via the respective data processing modules ~~(36,38)~~.

26. (Currently Amended)   The device of claim 23,~~24 or 25~~, wherein the data processing module ~~(36)~~ of the device includes means ~~(42)~~ for decrypting encrypted data received from the data processing module ~~(38)~~ of the data processing apparatus ~~(10)~~.

27. (Currently Amended)   The device of claim 23,~~24,25 or 26~~, wherein the data processing module ~~(36)~~ of the device includes means ~~(42)~~ for encrypting data transmitted to the data processing module ~~(38)~~ of the data processing apparatus ~~(10)~~.

28. (Currently Amended)   The device of claims 26 ~~or 27~~, wherein the ~~respective~~ data processing modules of the device ~~(36,38)~~ comprises a key for allowing ~~encryption and/or~~ decryption of data.

29. (Currently Amended)   The device of claim 28, wherein the key comprises a shared secret key for each of the respective data processing modules ~~(36,38)~~.

30. (Currently Amended)   The device of ~~any one of the preceding~~ claims 1, wherein the device is operatively coupleable to one of more of a plurality of said authentication storage means ~~(12)~~, each of which is registerable with a common telecommunication system ~~(16)~~, and wherein the authentication process is performed by a communications link ~~(19)~~ with the telecommunications system ~~(16)~~.

31. (Currently Amended)   The device of claim 30, in which the predetermined authentication information stored by each authentication storage means ~~(12)~~ corresponds to information which is used to authenticate a user of that authentication storage means in relation to the telecommunications system ~~(16)~~.

32. (Currently Amended)   The device of claim 31, in which each user is authenticated in the telecommunications system ~~(16)~~ by means of the use of a smart card or subscriber identity module ~~(e.g. SIM)~~, and in which the authentication storage means ~~(12)~~ respective to that user corresponds to or simulates the smart card for that user.

33. (Currently Amended)   The device of ~~any one of~~ claims 1 ~~to 32~~, in which the transaction is a transaction involving use of ~~the~~ data processing functions of the data processing apparatus.

34. (Currently Amended)   The device of ~~any one of~~ claims 1 ~~to 33~~, in which the authentication storage means ~~(12)~~ is specific to that device.

35. (Currently Amended)   The device of ~~any one of~~ claims 1 ~~to 34~~, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

36. (Currently Amended)   The device of ~~any one of~~ claims 30 ~~to 35~~, wherein the telecommunications system ~~(16)~~ includes means for levying a charge for the transaction when authorised.

37. (Currently Amended)   The device <u>of</u> ~~any one of~~ claims 1 ~~to 7, 16 and 17~~, wherein the security data entry means comprises a rotary knob.

38. (Currently Amended)   The device of ~~any one of the preceding~~ claim <u>1</u> in combination with the data processing apparatus.

39. (Currently Amended)   The device of ~~any one of the preceding~~ claims <u>1</u> in combination with the telecommunications system.

40. (Currently Amended)The device of ~~any one the preceding~~ claims <u>1</u>, wherein the authentication storage means communicates wirelessly to authenticate the transaction.

41. (Currently Amended)The device of ~~any one the preceding~~ claims <u>1</u>, wherein the authentication storage means (12) comprises a ~~smart card or SIM~~ <u>subscriber identity module</u> which authenticates the transaction when the ~~smart card or SIM~~ <u>subscriber identity module</u> is operable in a mobile terminal.

42. (Currently Amended)   The device of ~~any one the preceding~~ claim 30s, wherein the authentication storage means (12) comprises a <u>subscriber identity module</u> ~~smart card or SIM~~ which is further operable to authenticate a mobile terminal for use in the system.

43. (New)   The device of claim 8, wherein the device controls access to the predetermined information.

44. (New)   The device of claim 16, wherein the security data entry means comprises alphanumeric data entry means.

45. (New)   The device of claim 16, wherein the security data entry means comprises a keypad.

46. (New)   The device of claim 16, wherein the security data comprise a Personal Identification Number (PIN) and ~~analysing~~<u>analyzing</u> means compares the PIN obtained by the security data means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.

47. (New)   The device of claim 8, comprising a display for displaying security information.

48. (New)   The device of claim 8, comprising a data processing module for controlling the communication with the data processing apparatus .

49. (New)   The device of claim 48, wherein the data processing module of the device is configured for communicating with a corresponding data processing module of the data processing apparatus.

50. (New)   The device of claim 48, wherein communication between the authentication storage means and the data processing apparatus is performed via the respective data processing

modules.

51. (New)   The device of claim 48, wherein the data processing module of the device includes means for decrypting encrypted data received from the data processing module of the data processing apparatus.

52. ((New)   The device of claim 48, wherein the data processing module of the device includes means for encrypting data transmitted to the data processing module of the data processing apparatus.

53. (New)   The device of claims 52, wherein the data processing module of the device comprises a key for allowing decryption of data.

54. ((New)   The device of claim 53, wherein the key comprises a shared secret key for each of the respective data processing modules.

55. (New)   The device of claim 8, wherein the device is operatively coupleable to one of more of a plurality of said authentication storage means, each of which is registerable with a common telecommunication system, and wherein the authentication process is performed by a communications link with the telecommunications system.   /

56. (New)   The device of claim 55, in which the predetermined authentication information stored by each authentication storage means   corresponds to information which is used to authenticate a user of that authentication storage means in relation to the telecommunications system.

57. (New)   The device of claim 56, in which each user is authenticated in the telecommunications system by means of the use of a smart card or subscriber identity module, and in which the authentication storage means respective to that user corresponds to or simulates the smart card for that user.

58. (New)   The device of claim 8, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus.

59. (New)   The device of claim 8, in which the authentication storage means is specific to that device.

60. (New)   The device of claim 8, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

61. (New)   The device of claim 55, wherein the telecommunications system includes means for levying a charge for the transaction when authorised.

62. (New)   The device claim 16, wherein the security data entry means comprises a rotary knob.

63. (New)   The device of claim 8 in combination with the data processing apparatus.

64. (New)   The device of claim 8 in combination with the telecommunications system.

65. (New) The device of claim 8, wherein the authentication storage means communicates wirelessly to authenticate the transaction.

66. (New) The device of claim 8, wherein the authentication storage means comprises a subscriber identity module which authenticates the transaction when the subscriber identity module is operable in a mobile terminal.

	Application #	New Application
INFORMATION	Confirmation #	
	Filing Date	On even date herewith
DISCLOSURE	First Inventor	JEAL, et al.
	Art Unit	
STATEMENT	Examiner	
	Docket #	P08620US01/BAS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

S I R :

This IDS is submitted herewith pursuant to 37 CFR. §1.97-1.98 and includes the following:

☒ A **listing** of the references on PTO-1449.

☒ A copy of all **non-US** references which are listed on the PTO-1449 (US refs not required).

☒ A copy of a corresponding foreign **Search Report** which explains the relevance of the references noted therein.

☐ A separate **explanation of relevance**.

Please note the following particulars concerning the filing of this IDS:

☒ 1. This IDS is filed **within three months** of the filing date of a national application other than a CPA, or within three months of the date of entry into the national stage as set forth in 37 CFR. §1.491 in an international application, or before the mailing date of a first Office Action on the merits, or before the mailing of a first Office Action after the filing of a request for continued examination, whichever event occurs last.

☐ 2. This IDS is filed **after a first action,** but <u>before</u> a final action, allowance, or any other action which closes prosecution, **and:**
    ☐   **A.** Is accompanied by a payment in the amount of $180.00 required by 37 CFR. §1.17(p).
or
    ☐   **B.** I hereby state that each item of information contained in this IDS was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this IDS.
    ☐   **C.** I hereby state that no item of information in this IDS herewith was cited in a communication from a foreign patent office in a counterpart foreign application, and, to my knowledge after making reasonable inquiry, was known to any individual designated in 37 CFR. §1.56(c) more than 3 months prior to the filing of this IDS.
    ☐   **D.** An appropriate statement is attached.

- 1 -

☐ **3.** This IDS is filed **after** a final action or allowance, but on/<u>before</u> payment of the issue fee, **and**:

    ☐ **A.** is accompanied by a payment in the amount of $180.00 required by 37 CFR. §1.17(p).

and

    ☐ **B.** I hereby state that each item of information contained in this IDS was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this IDS.

    ☐ **C.** I hereby state that no item of information in this IDS herewith was cited in a communication from a foreign patent office in a counterpart foreign application, and, to my knowledge after making reasonable inquiry, was known to any individual designated in 37 CFR. §1.56(c) more than 3 months prior to the filing of this IDS.
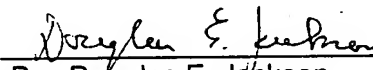
    ☐ **D.** An appropriate statement is attached.

☐ **4.** This IDS does not comply with 37 CFR 1.97-1.98, and is being filed **for placement in the file** pursuant to 37 CFR. §1.97(i)

☒ **5.** If no payment is enclosed and a fee is due in connection with this communication or if the payment enclosed is insufficient, the Commissioner is authorized to charge any fee or additional fee due with this communication to Deposit Account No. 12-0555.

Respectfully submitted,

Date: 4/15/05

By: Douglas E. Jackson
Registration No.: 28518

STITES & HARBISON PLLC ◆ 1199 North Fairfax St. ◆ Suite 900 ◆ Alexandria, VA 22314
TEL: 703-739-4900 ◆ FAX: 703-739-9577 ◆ CUSTOMER NO. 00881

- 2 -

Substitute for Form 1449A/PTO	Application #	New Application
	Confirmation #	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	On even date herewith
	First Inventor	Jeal et al.
	Art Unit	
	Examiner	
Sheet 1 of 3	Docket #	P08620US01

U.S. PATENT DOCUMENTS

Exam. Initial*	Document No. Number - Kind	Publ. Date MM-DD-YYYY	Name Patentee or Applicant	Relevance Passages/Figs.
	US-6,134,549		SHOWCASE	
	US-5,644,710		ETA	
	US-6,339,423		ENTRUST	
	US-6,161,182		LUCENT	
	US-6,229,806		MOTOROLA	
	US-2002/0087473		HARIF	
	US-6,154,839		VPNET	
	US-2001/045451	11/29/01	HSU ET AL	
	US-			

FOREIGN PATENT DOCUMENTS

Exam. Initial*	DOCUMENT Country-Number-Kind	Publ. Date MM-DD-YYYY	Name Patentee or Applicant	Relevance Passages/Figs.	Trans-lation
	WO 01/33936	5/17/01	PRIVACOMP INC.		
	EP 0 927 921	7/7/99	CASIO COMPUTER CO.		
	WO 00/67415	11/9/00	FIRST DATA CORP.		
	WO 02/039237	5/16/02	IIBM		
	EP 1 315 064	5/28/03	SUN MICROSYSTEMS		
	WO 02/079960	10/10/02	ENTERPRISES SOLUTIONS		
	GB 2 394 327	4/21/04	VODAFONE GROUP		
	WO 02/091316	11/14/02	ACTIVCARD		
	WO 03/084175	10/9/03	BARRACUDA INNOV.		
	WO 01/44950	6/21/01	SWIFTEYE, INC.		

NON PATENT LITERATURE DOCUMENTS

Exam. Initial*	Include NAME of the author (in CAPS), Title of Article/Item, Date, Page(s), Volume-Issue No., Publisher, City and/or Country where published	Trans-lation
	"Trusted Trasnaction Roaming"; pages 13-17, issue 1/2003- Secure; An Infineon Technologies Publication	

Examiner Signature		Date Considered	

* Examiner: Initial if considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.

223LT:20285:13613:1:ALEXANDRIA

Substitute for Form 1449A/PTO	Application #	New Application
	Confirmation #	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	On even date herewith
	First Inventor	Jeal et al.
	Art Unit	
	Examiner	
Sheet 2 of 3	Docket #	P08620US01

U.S. PATENT DOCUMENTS

Exam. Initial*	Document No. Number - Kind	Publ. Date MM-DD-YYYY	Name Patentee or Applicant	Relevance Passages/Figs.
	US-5,590,197	12/31/96	CHEN ET AL.	
	US-5,689,565	11/18/97	SPELMAN ET AL	
	US-6,449,651	9/10/02	DORFMAN ET AL	
	US-2002/129250	9/12/02	KIMURA	
	US-6,226,744		AT&T	
	US-6,230,002		ERICSSON	
	US-5,590,199		KRAJEWSKI	
	US-6,003,135		SPYRUS	
	US-			

FOREIGN PATENT DOCUMENTS

Exam. Initial*	DOCUMENT Country-Number-Kind	Publ. Date MM-DD-YYYY	Name Patentee or Applicant	Relevance Passages/Figs.	Trans- lation
	EP 1 229 476	8/6/02	SONY COMPUTER ENT		
	EP 1 022 638	7/26/00	IBM		
	FR 2793903	11/24/00	TELEDIFFUSION FSE		
	EP 1 223 524	7/17/02	AUTHENTURE, INC.		
	WO 97/46986	12/11/97	CKD SA		
	EP 0 715 242	6/5/96	NIPPON TELEGRAH		
	WO 01/82167	11/1/01	PHILIPSON		
	WO 01/26061	4/12/01	ABTRYGGIT		
	EP 1 043 648	10/11/00	SUN MICROSYSTEMS		
	GB 2 374 192	10/9/02	FREEDOM CARD LTD		
	EP 1 271 435	1/2/03	HEWLETT-PACKARD		

NON PATENT LITERATURE DOCUMENTS

Exam. Initial*	Include NAME of the author (in CAPS), Title of Article/Item, Date, Page(s), Volume-Issue No., Publisher, City and/or Country where published	Trans- lation
	"Dongles: Hardware Schutzt Software", Elektronik, Franzis Verlag Gmbh, Munchen, Germany; vol. 39, no. 10, 5/11/90 – pgs 82-84, 86.	

Examiner Signature		Date Considered	

* *Examiner: Initial if considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.*

223LT:20285:13613:1:ALEXANDRIA

Substitute for Form 1449A/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** Sheet 3 of 3	Application #	New Application
	Confirmation #	
	Filing Date	On even date herewith
	First Inventor	Jeal et al.
	Art Unit	
	Examiner	
	Docket #	P08620US01

U.S. PATENT DOCUMENTS

Exam. Initial*	Document No. Number - Kind	Publ. Date MM-DD-YYYY	Name Patentee or Applicant	Relevance Passages/Figs.
	US-5,754,646	5/19/98	WILLIAMS ET AL.	
	US-2002/069364	6/6/02	DOSCH	
	US-5,778 071	7/7/98	AMORUSO ET AL	
	US-6,226,744		MURPHY	
	US-			
	US-			

FOREIGN PATENT DOCUMENTS

Exam. Initial*	DOCUMENT Country-Number-Kind	Publ. Date MM-DD-YYYY	Name Patentee or Applicant	Relevance Passages/Figs.	Trans-lation
	EP 1 271 427 465	5/15/91	AT&T		
	EP 1 282 026	2/5/03	T.I.S.S.		
	WO 01/82167	11/1/01	PHILIPSON		
	FR 2 830 107	3/28/03	GEMPLUS SA		.
	EP 1 076 279	2/14/01	HEWLETT-PACKARD		
	EP 1 229 476	8/7/02	SONY COMPUTER ENT		
	EP 1288768	3/3/05	SIEMENS AG		
/	FR 2 793 575	11/17/00	SCHLUMBERGER SYSTEMS		/
	WO 00/31608	6/2/00	ERICSSON		
	WO 00/02407	1/13/00	NOKIA		
	WO 02/091316	11/14/02	ACTIVCARD		
	WO 01/80525	10/25/01	SUN MICROSYSTEMS		
	WO 00/70533	11/23/00	SCHLUM-BERGER SYS.		

NON PATENT LITERATURE DOCUMENTS

Exam. Initial*	Include NAME of the author (in CAPS), Title of Article/Item, Date, Page(s), Volume-Issue No., Publisher, City and/or Country where published	Trans-lation

Examiner Signature		Date Considered	

* *Examiner: Initial if considered, whether or not citation is in conformance with MPEP §609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.*

223LT:20285:13613:1:ALEXANDRIA

(51) International Patent Classification⁷: H04L 29/06, 12/22, G06F 1/00

(21) International Application Number:
PCT/GB2003/004377

(22) International Filing Date: 9 October 2003 (09.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0224228.7   17 October 2002 (17.10.2002)   GB
0307248.5   28 March 2003 (28.03.2003)   GB
0311729.8   21 May 2003 (21.05.2003)   GB

(71) Applicant (for all designated States except US): VODA-FONE GROUP PLC. [GB/GB]; Vodafone House, The Connection, Newbury, Berkshire RG14 2FN (GB).

(72) Inventors; and

(75) Inventors/Applicants (for US only): JEAL, David [GB/GB]; 8 Callow Croft, Burbage, Marlborough SN8

3TB (GB). MUDIE, George, Stronach [GB/GB]; 2 Lawrences Lane, Thatcham RG18 3LF (GB).

(74) Agent: MATHISEN, MACARA & CO.; The Coach House, 6-8 Swakeleys Road, Ickenham, Uxbridge UB10 8BZ (GB).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
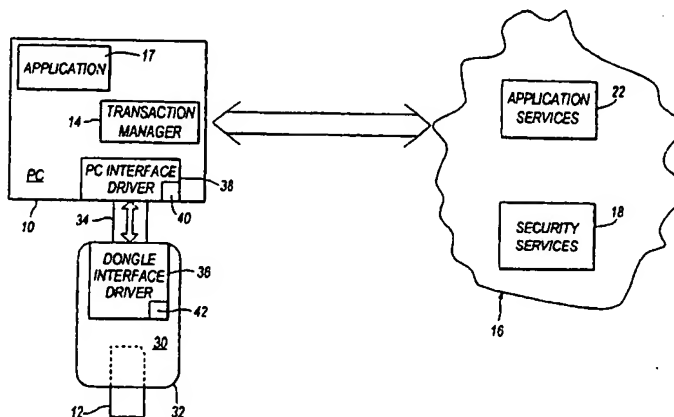
Published:
— with international search report

[Continued on next page]

(54) Title: FACILITATING AND AUTHENTICATING TRANSACTIONS

(57) Abstract: A device or "dongle" (30) is provided for controlling communications between a Subscriber Identity Module (or SIM) (12), such as of the type used in a GSM cellular telephone system, and a computer, such as a Windows-based PC (10). The SIM (12) can be authenticated by the telephone network, in the same way as for authenticating SIMs of telephone handset users in the network, and can in this way authenticate the user of the PC (10) or the PC (10) itself. Such authentication can, for example, permit use of the PC (10) for a time-limited session in relation to a particular application which is released to the PC (10) after the authentication is satisfactorily completed. The application may be released to the PC (10) by a third party after and in response to the satisfactory completion of the authentication process. A charge for the session can be debited to the user by the telecommunications network and then passed on to the third party. The dongle (30) provides additional security for the authentication data stored on the SIM by requiring a PIN to be entered and/or by only being responsive to requests received from the PC (10) which are encrypted using a key, which requests are generated by a special PC interface driver (38). The PIN may be stored only temporarily. The dongle (30) has an electrical connector (34), and means may be provided for selectively rendering the connector (34) available for coupling to the PC (10).

FACILITATING AND AUTHENTICATING TRANSACTIONS

The invention relates to the facilitation and authentication of transactions. In embodiments of the invention, to be described below in more detail by way of example only, transactions between data processing apparatus (such as a personal computer), or a user thereof, and a (possibly remote) third party are facilitated and authenticated, and such facilitation and authentication may also involve the facilitation and authentication of a payment or data transfer to be made by or on behalf of the user to the third party.

A method according to the invention of facilitating and authenticating transactions involving data processing apparatus such as a personal computer, and devices for connection to data processing apparatus (such as a personal computer) embodying the invention, will now be described, by way of example only, with reference to the accompanying diagrammatic drawings in which:

Figure 1 is a block diagram for explaining the operation of the method in relation to the data processing apparatus;

Figure 2 is a flow chart for use in the understanding of the block diagram of Figure 1;

Figure 3 is a block diagram corresponding to Figure 1 in which a "dongle" in accordance with the invention is used;

Figure 4 is a perspective view of one configuration of a dongle;

Figure 5 shows a side elevation of a further configuration of the dongle;

Figure 6 shows a block diagram for explaining the operation of a method of authenticating a transaction using data processing apparatus;

Figures 7A, 7B and 7C are a flow chart for use in understanding the authentication process carried out by the data processing apparatus of Figure 6.

Figure 8A shows a front view of a third configuration of a dongle;

Figure 8B shows a side view of the dongle of Figure 8A;

Figure 8C shows a cross-sectional view taken along line x-x of Figure 8B but with the

Figure 11C shows how the electrical connector emerges from the casing of the dongle.

In the figures like elements are generally designated with the same reference numbers.

There exist many instances when a transaction involving the use of data processing apparatus requires authentication. For example, the data processing apparatus may be required to carry out a transaction, such as the exchange of information, with a third party, such as a remote third party with which the communication must be made over a telecommunications link (including via the Internet). The third party may require that the data processing apparatus, or the user thereof for the time being, is authenticated to the satisfaction of the third party before the transaction takes place.

As stated, the transaction may merely involve the exchange of information. For example, the user of the data processing apparatus may simply need to be authenticated in order to download information from the third party. Such information may be information kept by the third party on behalf of the user of the data processing apparatus (for example, information relating to the user's bank account). Instead, the information might be information held on other data processing apparatus, such as a data network belonging to an organisation or commercial entity with which the user is connected or by whom the user is employed, thus facilitating access to that network by the user when the user is travelling. Another possible transaction may involve the downloading by the data processing apparatus of software from the remote location.

In addition, the transaction may require a payment to be made by the user in order to enable the transaction to take place, such as a payment to the third party in return for the information provided. Clearly, when such a payment is involved, it is important that the user is authenticated to the satisfaction of the third party and that the payment is made in a safe, simple and secure manner.

authentication process can be carried out. In a case where the SIM is the SIM of a subscriber to a particular cellular telecommunications network, the authentication process can be carried out by that network.

It should be noted that the authentication process being described does not necessarily authenticate the human identity of the user. For example, cellular telecommunication networks have pre-pay subscribers who are issued with SIMs in return for pre-payment enabling them to make calls on the network. However, the identity of such pre-pay subscribers is not known (or not necessarily known) by the networks. Nevertheless, such a user cannot make use of the network until the network has authenticated that user's SIM – that is, has confirmed that such user is a particular user who has a particular pre-paid account with the network. The SIMs of such pre-paid users or subscribers could equally well be used (in the manner described) in or in association with data processing apparatus or computers, for the purposes of authenticating that user.

The SIM need not take the form of a physical (and removable) smart card but instead can be simulated by being embedded in the data processing apparatus or computer in the form of software or represented as a chip for example.

It may be desirable to be able to change the authentication information on the SIM (or simulated SIM) to take account of changed circumstances. For example, the SIM may be a SIM registered with a particular cellular telecommunications network – a network applicable to the country or region where the data processing apparatus or computer is to be used. However, circumstances may arise (for example, the apparatus or the computer is physically moved to a different country or region) in which it is desirable or necessary to re-register the SIM with a different cellular telecommunications network. Ways in which this can be done are disclosed in our co-pending United Kingdom patent applications Nos. 0118406.8, 0122712.3 and 0130790.9 and in our corresponding PCT applications Nos. GB02/003265, GB02/003260 and GB02/003252. As described therein

The block diagram of Figure 1 schematically illustrates one way of operating the method described above.

A Windows-based personal computer or PC 10 is shown ('Windows' is a trade mark). The PC 10 is adapted to receive a SIM shown diagrammatically at 12. The SIM may be removably fitted to the PC, for use in identifying a user (that is, the holder of the SIM) or may be fixed within the PC (for identifying the PC itself). The PC 10 incorporates transaction management software 14 which interacts with and controls some of the functions of the SIM.

Although an arrangement has been described where the PC 10 is adapted to receive a SIM, it should be appreciated that a smart card other than a SIM might be used, and this is in accordance with the invention. Further, rather than the SIM (or smartcard) being received by the PC – by being removably fitted to the PC or fixed within the PC – the SIM (or smartcard) could be associated with the PC in any way that allows communication between the SIM (or smartcard) and the PC 10. For example, the SIM (or smartcard) could be provided with a "dongle" (examples of which are described hereinafter in detail) which allows wired or wireless communication with the PC 10. Preferably, the communication between the SIM (or smartcard) and the PC 10 is secure. The communications may be encrypted, or any other means for secure communication may be employed.

Also shown in Figure 1 is a cellular telephone network 16, such as the Vodafone (trade mark) network, and it is assumed that the SIM 12 is registered with the network 16.

The operation of the system shown in Figure 1 will be explained in relation to the flow chart of Figure 2.

At step A, the user of the PC 10 requests use of a particular application 17 on the PC. For

11

and from the SIM 12. There is no requirement for the transaction manager to be able to understand or interpret this data. The function of the transaction manager in the embodiment being described is to act as a conduit for the data being passed to and from the SIM 12.

The user can now make the request for the particular application (step H), accompanying this application request with the session key received at step G. The application request of step H is transmitted to an application services part 22 which may be part of the network 16 (as shown) or may be separate and controlled by a third party. At step I the application services part compares the session key received with the application request (step H) with the session key received at step F. Assuming that the result of this check is satisfactory, the application services part 22 now transmits acceptance of the application request (step J) to the PC 10, and the application now proceeds. The session key may allow time limited use of the application server 22, a single use or infinite use — depending on the circumstances. The network can now debit the user's account with a charge for the session. There may be communication link between the application services part 22 and the security services part 18 to allow data exchange between those parts — for example to allow the security services part 18 to arrange for the user's account with the network 16 to be debited.

The foregoing is of course merely one simple example of an implementation of what has been described.

In an alternative arrangement, a data carrier may be provided with means for storing predetermined information such as in one of the forms described above — that is, a SIM or (more probably) software simulating a SIM. The simulated SIM is associated with data stored on the data carrier. The data carrier may, for example, be a DVD or CD ROM or some other similar data carrier, and the data thereon may be software or a suite of software.

PC 10 or with reference to the network 16) so that decryption of the data is only performed up to the time specified in the licence sold with the data carrier.

Although a simulated SIM is described above, it is presently preferred that the SIM is implemented in hardware because this is more secure. The secret authentication data on a hardware SIM is inaccessible to unauthorised persons.

Rather than the PC10 being adapted to receive a SIM 12, or a data carrier being modified to incorporate a SIM or software simulating a SIM, a separate device or "dongle" 30 may be provided for receiving the SIM 12, or for incorporating software simulating the SIM 12.

Figure 3 shows a dongle 30 that allows data for authenticating a transaction (or for any other appropriate purpose) to be passed between the dongle 30 and the PC 10 and onwardly to/from the network 16.

The dongle 30 comprises a housing 32 having a slot for receiving a SIM 12. The housing 32 may be made of any suitable material. Preferably, this material is electrically insulating. For example, the housing may comprise laser activated resin or plastics.

Appropriate connectors (not shown) are provided within the housing 32 for allowing electronic exchange of data between the SIM 12 and the dongle 30. The dongle 30 further comprises a suitable connector 34 for allowing connection for data communication purposes to the PC 10. For example, the connector could be a USB connector, a Firewire 1394 connector or any other suitable connector. Of course, different configurations of the dongle may be provided. For example, the SIM 12 may be accommodated completely within the dongle 30, and may be removable from the dongle 30 by opening the housing 32, or the SIM 12 may be permanently sealed or encapsulated within the dongle casing 32. If the latter arrangement is provided, a user of the telecommunication system may be

sending data to or receiving data from the SIM 12.

Therefore, the PC interface driver 38 controls and supervises access to the dongle 30 and the SIM 12 to reduce the likelihood of the data stored on the SIM 12 being compromised by unauthorised attempts to access the SIM 12.

Provided that a request for access to data on the SIM 12 is approved by the PC interface driver (according, for example, to criteria set by the network 16), and is therefore communicated to the dongle interface driver 36 with the appropriate key 40, a transaction can be authenticated using the SIM 12 in the manner described in relation to Figures 1 and 2.

Although the provision of shared secret keys 40,42 is advantageous, it should be appreciated that the provision of shared secret keys 40,42 is not essential to the invention.

In an alternative arrangement the PC interface driver 38 is not provided with a particular secret key 40. However, the dongle interface driver 36 is provided with a key 42. When the dongle 30 is coupled to the PC 10 the PC interface driver 38 detects that the dongle interface driver is provided with a key 42. The PC interface driver 38 may then obtain from the network 16 via communications link 19 a key that will allow data exchange between the PC interface driver 13 and the dongle interface driver 36 encrypted using the key 42. For example, the key 42 of the dongle interface driver 36 may be a private key and the key 40 provided to the PC interface driver by the network 16 may be a public key – the two keys being a public-private key pair. The keys provided by the network 16 are preferably not provided on request by any application. For example, the network 16 may be configured to only provide these keys to a trusted PC interface driver and/or after some authentication process.

Alternatively, the data transfer between the dongle interface driver 36 and the PC

transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 12 is performed within the dongle 30, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC10. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorised party.

To allow entry of the PIN the dongle 30 requires a power supply. Power can be provided by the PC 10. Advantageously, the PIN has its own temporary power supply which allows the PIN to be entered and verified. Subsequently, the power supply is interrupted and the PIN data is lost. This is an additional security feature, and is described in more detail below.

The PIN entry comparison arrangement of Figure 4 may be provided in addition to or as an alternative to the interface drivers 36,38 and shared secret keys 40,42 of the arrangement shown in Figure 3.

It should be appreciated that as an alternative to push buttons 46, other means could be provided for allowing PIN entry. Alternatively, the user could be authorised to use the SIM by obtaining some other security information from the user and comparing this with data stored on the SIM 12. For example, the data obtained could be the user's fingerprint or some other characteristic which is unlikely to re-occur on another person – for example, any suitable biometric data. The details of the fingerprint (or other information) are stored on the SIM for comparison with the input data representing the characteristics.

As an additional security feature in the Figure 4 embodiment, a display may be provided which displays the name of the application or organisation which requests information from the SIM 12. This would allow the user to monitor requests being made to his SIM 12.

configured vending machine or tickets to be purchased from an appropriately configured ticketing machine. Such machines will include a processor so that the functions corresponding to those performed by the transaction manager 14 of the PC 10 can be performed by the machines.

In the above description it has been indicated that the SIM used to authenticate the transaction could have the form of a conventional SIM which is either inserted in an appropriate slot within the PC 10 or in the dongle 30 (if provided). This could simply be the SIM that a subscriber to a mobile network uses in their conventional mobile terminal to make and receive calls. Alternatively, the SIM 12 could be embedded within the PC 10 or the dongle 30 (such that it cannot be readily removed or cannot be removed at all). Further alternatively, the SIM may not have a separate physical form, but may be simulated by means of software and/or hardware within the PC 10 or the dongle 30. The SIM could be simulated or incorporated into the chip set of the PC 10. For example, the SIM could be incorporated or simulated within the central processor unit of the PC 10. Such an arrangement prevents the SIM (or simulated SIM) being removed from the PC 10 (other than by rendering the PC 10 useless).

If the SIM is of a form that is not readily removable from the PC 10 or dongle 30, a subscriber to the telecommunications system may be provided with a second SIM for use, for example, in their mobile telephone handset.

If, however, the same SIM is used (in the PC 10 or the dongle 30) to authenticate transactions and for use in the conventional manner with the telecommunications network (for example, to make and receive calls using a mobile telephone), the same data may be used to provide authentication of transactions as is used to authenticate the SIM with the mobile telephone network when a call is being made. Alternatively, the SIM may have separate records for performing each authentication type. There may be a first record containing data and/or algorithms for use in authenticating transactions, and a second,

the software would cause appropriate signals to be sent to the dongle 30 to change the active SIM, simulated SIM or data record.

As an added security measure, the dongle may require the subscriber to enter a PIN (or provide other data) in order to activate different modes of the SIM (e.g. "employee" mode or "personal" mode). A different PIN could be required to activate each mode.

The dongle 30 thus far described has a physical connector 34 (such as a USB connector) to enable data communication with a PC10. As an alternative to a physical connector 34, a wireless link between the dongle 30 and the PC 10 may be provided. Data exchange may take place, for example, by using near field techniques, using Bluetooth technology, by infra-red signalling or any other suitable means.

Rather than a separate dongle 30 being provided, a user's SIM may be located in a mobile terminal (such as a mobile telephone handset) in the conventional way. The SIM may authenticate transactions with the PC 10 by suitable data exchange between the mobile terminal and the PC 10. This could be achieved by providing the mobile terminal with a physical connector (such as a USB connector) to connect the PC 10 when authorisation of a transaction is required, or could be done by any of the wireless techniques described above. Preferably, this communication is encrypted or made secure in some other way. If the SIM is provided with separate data records for conventional mobile telecommunications purposes and for authorising transactions, it may be possible to simultaneously make a telephone call, for example, with the telecommunications network and authenticate a transaction with the PC 10. The mobile terminal may conveniently provide the communication link between the PC 10 and the network 16. The coupling of the mobile terminal to the PC 10 therefore in this arrangement not only allows authentication of transactions but also conveniently provides a communication medium between the PC 10 and the network 16. In an alternative arrangement, the mobile terminal still provides communication over a mobile telecommunications network, but

100, such as SMS, MMS, location based services, etc. The network 16 also provides an authentication service 102 and a payment service 104. However, it should be understood that the network may be any type of network – the invention is not restricted to mobile telecommunication networks. For example, the authentication service 102 and payment service 104 may be provided in a computer that is linked to PC 10 by a local area network, a wide area network and/or the Internet.

When the subscriber wishes to use a service provided by a remote service provider 22 (step A of the flow chart shown in Figure 7A), the subscriber couples their SIM 12 to the PC 10 by inserting their dongle 30 containing the SIM 12 into the appropriate connecting slot of the PC 12 or using a wireless link (step B). The subscriber then activates on the PC 10 the relevant client application 17 to obtain a required service (step C). For example, the client application 17 could be special software provided by or under control of a service provider 22 for installation on the subscriber's PC 10. Alternatively, a client application 17 might be a web browser for visiting an appropriate web site of the service provider 22.

To illustrate the operation of the system shown in Figure 6, an example will be given for a subscriber wishing to purchase a particular CD from a vendor which is a service provider 22. Using a graphical user interface present on the PC 10 the subscriber launches web browser software provided on the PC 10 and, via the Internet, accesses the web site of the service provider 22. The web browser software constitutes the client application 17, and allows access to the web site associated with the service provider 22 which distributes CDs.

Data communication between the client application 17 and the service provider 22 may be by a fixed network (e.g. PSTN) or by a wireless network – such as the network 16 or another mobile telecommunications network.

- ADDRESS

- PREFERENCES

- BANK ACCOUNT DETAILS

o FOR Service Provider C

- NAME

- ADDRESS

- PREFERENCES

- BANK ACCOUNT DETAILS

As well as the network 16 storing the data relating to a subscriber's SIM and their MSISDN, the network 16 also includes a list of pseudonyms that the subscriber has established with various service providers (service providers A,B,C,...). The information stored for any particular service provider may be different, and will depend upon what information the service provider might usefully require from the subscriber and upon the information that the subscriber is willing to provide to the service provider. In the example shown, the pseudonym might include details of the name and address of the subscriber and any preferences that they may have relating to the particular service. In the example of a subscriber wishing to purchase a CD from service provider 22, this might include the subscriber's preference for a particular type of music, allowing the service provider to tailor its service, perhaps to offer the subscriber CDs relating to a type of music that the subscriber prefers.

When the user accesses the website, the service provider 22 will cause the subscriber as part of the login procedure to be prompted, using the web browser, to enter a "pseudonym" which that subscriber may have previously registered with the service provider 22 (step D). If a pseudonym has been previously registered by that subscriber with the service provider 22, the subscriber enters their pseudonym and this is sent by the client application 17 (step E) to the service provider 22. The service provider 22, by

subscriber uses when obtaining services from their physician but would not wish this information to be made available to other service providers.

The subscriber searches the web site to identify the CD that the subscriber wishes to purchase. When the CD required by the subscriber is identified, the subscriber causes the client application 17 to send a request for service message to the service provider 22 (step H) – for example by making a mouse click on a "purchase CD" button provided by the web site. The message includes data identifying the CD required, data identifying the subscriber (such as the subscriber's SIM identifier), including a field indicating that the subscriber has installed on their PC a transaction manager 14 which can authenticate a transaction by means of the subscriber's SIM 12.

At this stage in the transaction, the service provider 22 has been provided with certain details of the subscriber, including the subscriber's name, address and the CD that they wish to order. This information might be provided by somebody who is not truly the subscriber. To authenticate the transaction the service provider 22 constructs a service context S_C (step I). The service context is a data packet including the following fields:

- o An identifier of the service provider 22
- o The subscriber's name (or other identifier such as a SIM identifier)
- o Details of the transaction to be authenticated (in this case the purchase of a CD)

Additional or alternative information may of course also be provided.

The service context S_C is sent via the Internet to the client application 17. The client application 17 passes the service context S_C to the transaction manager 14 (step J). The client application 17 may add its own identifier to the service context S_C to allow the network 16 to determine from which client application the transaction is derived.

applications/organisations by entering the user's PIN using a keypad, or by providing other identifying data.

The subscriber will thereafter be authenticated by the authentication service 102 performing a challenge and response session with the SIM (by sending data via the transaction manager 14) –step M. For example, the authentication service 102 will send a random challenge to the transaction manager 14, which is transmitted to the SIM. The SIM responds by encrypting the random challenge using both an authentication algorithm and a unique key Ki resident within the SIM and assigned to that particular subscriber. The response is transmitted by the transaction manager to the authentication service 102. The authentication service 102 analyses the response to determine whether it is the response that would be expected from that subscriber's SIM. If the response is as expected, then the authentication service 106 issues a security token S_x and sends this to the transaction manager (step N). The transaction manager 14 itself need not understand the data exchanged during the challenge and response procedure – it merely acts as a conduit for this data.

As described in relation to Figure 3, to prevent, or to reduce, the likelihood of the transaction manager 14 being replaced or bypassed by an alternative application, which could compromise the security of the data on the SIM 12, the transaction manager 14 and the dongle interface driver may be provided with respective shared secret keys. Each communication from the transaction manager 14 to the dongle 30 is then encrypted using the shared secret key 40. All communications from the PC 10 to the dongle 30 are received by the dongle interface driver. The dongle interface driver comprises processing means for decrypting received communications using its secret key. To enhance security, the dongle interface driver will prevent all communications other than those encrypted using the shared secret key from sending data to or receiving data from the SIM 12.

Therefore, the transaction manager 14 controls and supervises access to the dongle 30 and

The client application 17 then passes the security token to the service provider 22 (step P).

The security token S_X includes data specific to a particular subscriber and a transaction with a particular by the service provider 22. Numerous transactions may be handled by the network 16, transaction manger 14 and service provider 22 in parallel. These will be distinguishable from one another by virtue of the data specific to a particular transaction with a particular by the service provider 22 in the security token S_X.

If the security token S_X is intercepted as it passes between the network 16 and the transaction manager 14, or between the client application 17 and the service provider 22, it will have no value to the interceptor. The security token S_X is specific to particular transaction with a particular by the service provider 22, and the provision of a service to a particular subscriber.

On receipt of the security token S_X by the service provider 22 its content is analysed and, if it is established that it corresponds to a service context Sc issued by the service provider 22, the service provider 22 may assume that the request for service (order of a CD) is legitimately made by the subscriber. The Service Provider 22 could present the Security Token Sx to the Authentication Service 102 to check the validity of the token. The authentication service 102 then checks the integrity of the Security Token Sx and validates the content of the Security Token Sx. The authentication service 102 then sends a response to the service provider 22 indicating that the Security Token Sx is valid. Alternatively, the authentication service 102 may send data to the service provider 22 that allow the service provider 22 itself to determine the integrity and validity of the Security Token Sx.

The service provider 22 then determines whether a payment needs to be made (step Q). If no payment is required the CD can then be despatched. However, if a payment is required, the service provider 22 then generates a payment context P_C which includes the

network 16.

Advantageously, if the user has a pseudonym associated with the service provider 22, the service provider 22 may update that pseudonym on the basis of any new information learnt about the subscriber from the transaction – for example, a change in music taste.

The communications between the PC 10 and the network 16 are preferably encrypted, as described above. It is also preferable for communications between the components within the PC 10 and within the network 16 to be encrypted – for example by use of shared keys.

In the arrangement described above, the subscriber is authenticated only when they wish to purchase a CD. In an alternative arrangement, the subscriber may be authenticated when they log onto the web site. The service provider will then have a security Token Sx relating to that subscriber's session with the web site. When the subscriber wishes to make a purchase, the Security Token Sx is sent to the authentication service 102. The authentication service 22, depending on the value of the purchase, for example, my either validate the Security Token Sx or require the service provider 22 to obtain a further security token via the client application 17, transaction manager 14 in the manner described above. Any pseudonym data relating to that subscriber and for that service provider 22 can be provided to the service provider 22 upon authentication of the subscriber.

The Security Token Sx may be valid for a limited time period. The SIM is advantageously provided with means for accurately determining the true time – for example with a tamper-resistant internal clock, a clock provided by the PC 10, or a time indication from the network 16 (which will be a "trusted" time).

The subscriber may obtain network services 100 from the network 16 in a similar manner to the way in which services are obtained from the service provider 22. That is, the

35

A further example of the use of this system will now be described in relation to the renting of a vehicle. A subscriber to network 16 couples their dongle to a PC 10 (or other processing device) at the offices of the vehicle rental company. The PC 10 includes the transaction manager 14 and a client application 17 for providing access to the vehicle rental service provider 22.

If the subscriber has a pseudonym for use with the service provider 22, the subscriber will provide this to the service provider 22, which is then able to access relevant data relating to the subscriber from the authentication service 102 of the network 16. If the subscriber does not have a pseudonym associated with the service provider 22, the user provides relevant details when prompted by the service provider 22, such as the subscriber's name, address, the type of vehicle they wish to rent and the duration of the rental period.

The service provider 22 then creates an appropriate service context S_C and transmits this to the client application 17. The transaction manager 14 receives the service context S_C and passes this to the authentication service 102 of the network 16 to seek a security token S_X following authentication of the transaction by the challenge and response procedure performed between the authentication service 102 and the SIM 12 via the transaction manager 14 in the manner described above. If the SIM 12 is authenticated by the authentication service 102 of the network 16, a security token S_X is issued to the transaction manager 14. The security token S_S is passed to the client application 17, and from there to the service provider 22 to authenticate the transaction.

By means of a link 105 between the authentication service 102 and the payment service 104, appropriate funds can be reserved from the subscriber's account with the network 16. For example, funds may be reserved to cover the expected rental charges and possibly a deposit.

the vehicle rental company service provider 22 (possibly using information from the vehicle systems as described above), and an appropriate payment context P_C is generated and transmitted to the client application 17 present on PC 10 (which could be a different PC from the PC 10 used to initiate the transaction with the vehicle rental company. The transaction manager 14 of the PC 10 then receives the payment context P_C and obtains from the payment service 104 of the network 16 a payment token P_X. This is passed to the service provider 22 via the transaction manager 14 and client application 17, and the service provider 22 is then able to collect the appropriate payment from the payment service 104 of the network 16.

In a further example, the transaction manager 14 and the client application 17 are provided in a vehicle as part of the vehicle's on-board telecommunication system. The vehicle, for example in a convenient position on the dashboard, includes a connector to receive a subscriber's dongle 30 (although, of course, a wireless connection could alternatively be provided). When the subscriber inserts the dongle 30, access to remote services provided by service providers 22 may be obtained using the transaction manager 14 and client application 17 in the manner described in relation to Figures 6 and 7.

Because the vehicle is, of course, mobile, communications between the client application 17 and the remote service provider 22 and communications between the transaction manager 14 and the authentication service 102 and the payment service 104 (or between the client application 17 and the network service 100) will be provided by a wireless link, such as by use of a mobile or cellular radio network using a telephone transceiver already present in the vehicle. The network used to perform these communications may be the same as the network 16 providing the authentication and payment services 102 and 104, or may be a different network.

While inserting the dongle 30 into the connector of the vehicle, the user may also be able to make and receive telephone calls in the usual manner as if the user had inserted their

The service provider, being sure that the subscriber or payment is authenticated, is then able to despatch the CD to the subscriber.

In order to obtain payment the service provider 22 may proceed in one or two ways.

In the first procedure the service provider 22 issues a request for payment clearance by sending a data packet including the payment token P_x (and the Security Token S_x) to the client application 17. The client application 17 passes the payment clearance request to the transaction manager 14, which in turn passes the payment clearance request (with the payment token P_x) to the payment service 104. At this point the payment service may instruct the authentication service 102, via link 105, to authenticate the subscriber by challenge and response data exchanged with the SIM 12 (via the transaction manager 14), although this is an optional step. In any event, the payment service 104 checks the payment token P_x and the security token S_x (contained in the same packet) and then clears funds in the subscriber's account with the network 16. The payment service 104 then sends a modified payment token P_{x1} to the transaction manager 14. The transaction manager 14 passes the modified payment token P_{x1} to the service provider 22 via the client application 17. The service provider 22 is then able to validate the payment token by direct link 108 with a payment service 104.

As an alternative to the procedure described above, the service provider 22 may request the payment service 104 for payment clearance via link 108 by sending the appropriate payment token P_x. The payment service 104 then validates the payment token and clears the funds. The payment service 104 responds to the service provider 22 confirming that the payment has been cleared.

Figures 8 to 11 show further examples of dongle configurations that could be used in conjunction with the systems described in relation to Figure 1 or 6 as an alternative to the

movable between a first position, shown in Figures 9A and 9B, where it is contained completely within the casing of the dongle 270, and a second position, shown in Figures 9C and 9D, where the connector 254 is shown extending from the casing of dongle 270. However, in the third configuration, the linear movement of the electrical connector 254 in the direction of arrow 268 is provided by rotating knob 272 with respect to the casing of dongle 270 as shown by arrow 274. Rotation of the knob 272 in a first direction causes the connector 254 to emerge from the casing of dongle 270, and rotation in the opposite direction causes the connector 254 to be retracted within the casing of the dongle 270. Any suitable mechanism for converting the rotary motion of the knob 272 into linear motion of the connector 254 may be provided. For example, a mechanism described in U.S. Patent No. 5813421 (which is incorporated herein by reference) for a lipstick swivel mechanism may be employed. Other suitable mechanisms will be known to those skilled in the relevant art.

The dongle 270 includes a display 248 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered. The dongle 270, rather than having a series of push buttons (such as a numerical key pad) comprises a data entry knob 276 which is mounted to the dongle for rotation as shown by arrow 278 and also for linear motion with respect to the dongle as shown by arrow 280. Each digit of the PIN number is input by the user grasping the knob 276 and pulling it in a direction away from the casing of the dongle 270 (in the direction of arrow 280). An indication, such as a flashing cursor then appears on the display 248 indicating that the first digit of the PIN number is expected. The number is input by rotation of the knob 276 (arrow 278), the displayed number increasing in value with further rotation of the knob 276. When the required number appears on the display 248 the user confirms that this is the number they wish to input by pushing the knob 276 in the opposite direction to arrow 280. To input the next digit of the PIN number the knob 276 is again lifted (arrow 280) and the correct number is selected by rotation of the knob. The required number is entered by returning the knob 276 to its original position by moving it in the direction opposite to the arrow 280. This

292. In this embodiment, the first digit of the user's PIN number is entered by rotating the knob 96 until the correct digit of the PIN number (indicated at 300) is aligned with the mark 302. When the relevant digit and the mark 302 are aligned, the user stops rotation of the knob 296. When movement of the knob 296 stops, the position of the knob 296 is recorded by the dongle 290 so that the digit of the PIN number can be detected. The next digit of the PIN number is entered by rotating the knob 296 in an anti-clockwise direction (opposite to arrow 298) until the relevant digit of the PIN number is aligned with marking 302. Again, when the rotation of the knob stops, the position of the knob is recorded so that the PIN number can be recorded by the dongle 290. The next digit of the PIN number is entered by clockwise rotation of the knob 296, and so on, until all of the digits of the PIN number have been entered. The manner of data entry using the knob 296 and the marking 302 is similar to that used to enter the combination of a safe.

The dongle 290 further includes an optional digital camera 304 mounted at the axis of rotation of the knob 296 (but fixed with respect to the main body 292). Dongle 290 includes processing means and memory for storing one or more images captured by the camera 304, and allows these images to be transferred to the PC 10 using the connector 254.

Figures 11A to 11C show a sixth configuration of a dongle 310. The dongle 310 comprises a casing 312 which has an opening 314 at one side thereof. Contained within the casing 312 is a coupling portion 316 to which the electrical connector 254 is fixed. The coupling portion 316 is connected to the casing 312 in such a manner that the coupling portion 316 is rotatable about an axis indicated by dotted line 318.

Connected to the loop connector 244 is a ring 320, which provides a convenient means by means a slidable part 322, which is mounted for sliding with respect to the casing 312, may be moved with respect to the casing 312 in the direction of arrow 324. By means of a rack and pinion or any other suitable mechanism (not shown) the movement of the

45

employed, the provision of a movable electrical connector 254 will not be necessary.

The dongles of Figures 8 to 11 may or may not include the dongle interface driver 36 described in relation to Figures 3 and 4.

The dongles of Figures 9 and 10 may allow the PIN to be passed to the PC 10 for validation, or such validation may be performed within the dongle for improved security.

Of course, the dongles of Figures 8 and 11 may be provided with a PIN entry means if required.

7. · The device of any one of claims 1 to 6, comprising means for analysing the entered security data for determining whether to allow access to the predetermined information.

8. A device for connection to a data processing apparatus, the device including first coupling means for operative coupling to authentication storage means storing predetermined information relating to the authentication of a transaction with the data processing apparatus; second coupling means for operative coupling to the data processing apparatus; and configuration means for selectively rendering the second coupling means available for coupling to the data processing apparatus, the device when operatively coupled to the data processing apparatus being responsive to an authentication process carried out via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined configuration information.

9. The device of claim 8, wherein the configuration means comprises means for selectively making the second coupling means available externally of the device housing.

10. The device of claim 9, wherein the configuration means comprises a removable cap.

11. The device of claim 9, wherein the configuration means comprises a closure member coupled to and moveable with respect to the housing for selectively closing an aperture in the housing.

12. The device of claim 11, comprising interconnection means for connecting the closure member and the second coupling means, the arrangement being such that, as the closure member is moved to open the aperture, the second coupling means emerges from the aperture.

13. The device of claim 8, comprising a knob mounted on the device housing for

entry means comprises a keypad.

21. The device of any one of claims 1 to 7 and 16 to 20, wherein the security data comprise a Personal Identification Number (PIN) and analysing means compares the PIN obtained by the security data means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.

22. The device of any one of the preceding claims, comprising a display for displaying security information.

23. The device of any one of the preceding claims, comprising a data processing module for controlling the communication with the data processing apparatus.

24. The device of claim 23, wherein the data processing module of the device is configured for communicating with a corresponding data processing module of the data processing apparatus.

25. The device of claim 24, wherein communication between the authentication storage means and the data processing apparatus is performed via the respective data processing modules.

26. The device of claim 23,24 or 25, wherein the data processing module of the device includes means for decrypting encrypted data received from the data processing module of the data processing apparatus.

27. The device of claim 23,24,25 or 26, wherein the data processing module of the device includes means for encrypting data transmitted to the data processing module of the data processing apparatus.

35. The device of any one of claims 1 to 34, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

36. The device of any one of claims 30 to 35, wherein the telecommunications system includes means for levying a charge for the transaction when authorised.

37. The device for any one of claims 1 to 7, 16 and 17, wherein the security data entry means comprises a rotary knob.

38. The device of any one of the preceding claims in combination with the data processing apparatus.

39. The device of any one of the preceding claims in combination with the telecommunications system.

40. The device of any one the preceding claims, wherein the authentication storage means communicates wirelessly to authenticate the transaction.

41. The device of any one the preceding claims, wherein the authentication storage means comprises a smart card or SIM which authenticates the transaction when the smart card or SIM is operable in a mobile terminal.

42. The device of any one the preceding claims, wherein the authentication storage means comprises a smart card or SIM which is further operable to authenticate a mobile terminal for use in the system.

APPENDIX B

UPS Uni

Log-In   User ID: _____   Password: _____ | | Forgot Password

Tracking

→ **Track by Tracking Number**
  > Track by E-mail
  > Import Tracking
    Numbers 🔒
→ Track by Reference Number
→ Track by Freight Tracking
  Number
→ Track by Freight Shipment
  Reference
→ Track with Quantum View
→ Sign Up for Signature
  Tracking 🔒
→ Void a Shipment 🔒
→ Help

Track by Tracking Number

View Details

Status:	Delivered
Delivered on:	08/01/2006 11:08 A.M.
Signed by:	LONG
Location:	NEXT DOOR
Delivered to:	WEST BERKSHIRE, GB
Shipped or Billed on:	07/28/2006
Tracking Number:	1Z Y48 R60 66 9939 460 2
Service Type:	EXPRESS

Package Progress:

Location	Date	Local Time	Activity
ABINGDON, GB	08/01/2006	11:08 A.M.	DELIVERY
	08/01/2006	4:38 A.M.	IMPORT SCAN
	08/01/2006	4:37 A.M.	OUT FOR DELIVERY
ABINGDON, GB	07/31/2006	2:45 P.M.	THE RECEIVER WAS UNAVAILABLE ON THE 1ST DELIVERY ATTEMPT. A DELIVERY ATTEMPT WILL BE MADE
	07/31/2006	7:48 A.M.	IMPORT SCAN
	07/31/2006	7:47 A.M.	OUT FOR DELIVERY
EAST MIDLANDS AIRPOR, GB	07/31/2006	12:28 A.M.	IMPORT SCAN
EAST MIDLANDS AIRPOR, GB	07/30/2006	10:16 P.M.	ARRIVAL SCAN
PHILADELPHIA, PA, US	07/30/2006	10:42 A.M.	DEPARTURE SCAN
PHILADELPHIA, PA, US	07/29/2006	8:08 A.M.	ARRIVAL SCAN
LOUISVILLE, KY, US	07/29/2006	6:27 A.M.	DEPARTURE SCAN
	07/29/2006	12:14 A.M.	ARRIVAL SCAN
CHANTILLY, VA, US	07/28/2006	10:44 P.M.	DEPARTURE SCAN
	07/28/2006	10:07 P.M.	ARRIVAL SCAN
ALEXANDRIA, VA, US	07/28/2006	9:25 P.M.	DEPARTURE SCAN
	07/28/2006	9:14 P.M.	ORIGIN SCAN
	07/28/2006	4:44 P.M.	PICKUP SCAN

US   07/28/2006   4:25 P.M.   BILLING INFORMATION RECEIVED

Tracking results provided by UPS: 08/01/2006 3:08 P.M. Eastern Time (USA)

NOTICE: UPS authorizes you to use UPS tracking systems solely to track shipments tend
for you to UPS for delivery and for no other purpose. Any other use of UPS tracking syste
information is strictly prohibited.

←Back to Tracking Summary

Schulman, B. Aaron

From: Mudie, George [George.Mudie@bskyb.com]

Sent: Tuesday, August 15, 2006 4:00 AM

To: Schulman, B. Aaron

Subject: RE: P08620US01/BAS

Dear B. Aaron Schulman,

I have received a request from Stites & Harbison PLLC this morning, requesting that I sign a Declaration for Utility or Design Patent application. As you can see from my details I no longer work for Vodafone (in fact I left over two years ago). I also believe that I signed something similar a couple of months ago, this was sent to me by a solicitor based at the Vodafone HQ in Newbury.

I'm not sure I see the need to sign another declaration, as I've received no reward or recognition from Vodafone for this invention.

Yours sincerely,

George Mudie
Director of Customer & Interactive Technology
Sky

Tel: 0207 800 2587
Fax: 0207 805 7347
E-Mail: george.mudie@bskyb.com

Registered office: British Sky Broadcasting Limited, Grant Way, Isleworth, Middlesex, TW7 5QD
Registered in England No 2906991

8/15/2006

(Registration No. 2340150) are direct or indirect subsidiaries of British Sky Broadcasting Group plc (Registration No. 2247735). All of the companies mentioned in this paragraph are incorporated in England and Wales and share the same registered office at Grant Way, Isleworth, Middlesex TW7 5QD.